FORSVARSAKADEMIET

BRIEF

CYBER DETERRENCE - A 21st CENTURY MAGINOT LINE

By MSc Thomas Thomasen,
Institute for Strategy

FORSVARET

FORSVARSAKADEMIETS FORLAG

BRIEF

CYBER DETERRENCE - A 21st CENTURY MAGINOT LINE

By MSc Thomas Thomasen,
Institute for Strategy

Thomas Thomasen works at the Royal Danish Defence College – Institute for Strategy. He holds an MSc in Theory and History of International Relations from the London School of Economics and Political Science.

Thomas Thomasen can be contacted via mail: ifs-un04@fak.dk

Institute for Strategy - ifs@fak.dk
Faculty of Strategy and Military Operations
Royal Danish Defence College PO Box 2521 DK-2100 Copenhagen

The Royal Danish Defence College is the Danish armed forces' powerhouse for education, training and research-generated consultancy. Our research is conducted within a broad range of military-related topics. Our research priorities, such as topics and resource allocation are determined by the Commandant of the Royal Danish Defence College, who is aided by a research council.

Research at the Royal Danish Defence College should enlighten and challenge the reader, whether they are in the armed forces or in the surrounding environment. This is only achievable if the employees have the freedom to administer their own research projects and draw their own conclusions. This is a principle, which is honoured at the Royal Danish Defence College.

We hope you enjoy reading the Royal Danish Defence College's publications!

Copenhagen September 2011
Royal Danish Defence College
Ryvangs Allé 1
DK-2100 Copenhagen
Denmark
Phone: +45 3915 1515
Fax: +45 3929 6172
Editor: Director of the Institute for Strategy Ole Kværnø
Layout by B-O. Kure
ISBN: 978-87-987720-8-8

Royal Danish Defence College Publishing House

Introduction

The Maginot Line was a defensive line along the Franco-German border. When it was finished in 1939, it was thought to provide an impregnable defence against the rising military might of Nazi Germany. One year later, German forces invaded France through Belgium, rendering the grand Maginot Line irrelevant. The fortification line has since been a symbol of strategies that provide a false feeling of security in times of great anxiety. Today, we live in a time of great anxiety – as the former US President Clinton put it: "face a world of endless risk." One such risk is the multitude of threats that we are faced with in cyberspace. This brief will make the case that deterrence in cyberspace is a 21st century Maginot Line.

Cyber security attempts to mitigate the effects of "malicious manipulation of cyber systems (...)."[1] It is among the top tier threats faced by states in the contemporary international security landscape. Ralph Langner's concept of cyber systems, in the definition above, encapsulates the width and depth of technology in Western societies. For example, it includes the Internet, software, hardware and industrial control systems such as SCADA. Cyberspace thus covers more than merely the Internet that we use every day or 'visible' electronic components such as ATMs – it is everything that features an electronic component. In essence, it is the body of electronic objects that underpin our modern societies.

This underpinning reinforces the strategic importance of cyberspace. It is particularly pertinent due to the network centric character of contemporary society. Our reliance on networks and cyber systems for purposes of communication, air traffic control, international trade and power grid management demonstrates this network centrism. The critical infrastructure that is vital to any modern economy and national security relies to an increasing extent on a 'system of systems'. Securing cyber systems thus goes to the very heart of national security. This trend appears only to be growing with the pace of technological development and the further integration of technology into various central functions in society. The benefits of this integration are matched by equally grave challenges. It is thus no surprise that cyber security has risen to the very top of the international security agenda.

Nevertheless, it is only recently that cyber security has gained credibility as a top tier threat to national security. This is largely due to a series of high profile events. In April 2007, as Estonian authorities began moving a Soviet World War II memorial, riots broke out in the streets of Tallinn. This was not surprising, given the historical and political background of Estonia's significant Russian minority, but what followed was: a month-long siege on Estonia's cyber infrastructure, which resulted in the shutdown of government and financial online services.[2] Being one of the most 'wired' states in the world, this was a significant disruption to a society dubbed "E-stonia." In the time since 2007, the perception of cyber attack as a top

(1) Ralph Langner, 9 June 2011, International conference on Cyber Conflict, Tallinn, Estonia

(2) Landler, M. and Markoff, J. (2007) "Digital Fears Emerge After Data Siege in Estonia" *New York times, 29 May 2007.*

tier threat has been further reinforced by a series of incidents: The Stuxnet worm that successfully targeted Iran's nuclear programme, as well as intellectual property theft from the Joint Strike Fighter Programme and Google. These incidents have illustrated both the utility and threat posed by cyber weapons. Stories of these incidents have been circulating widely in the media, but they are only the tip of the iceberg. In a recent publication co-authored by The Center for Security and International Studies (CSIS) and McAfee, critical infrastructure owners reported that attacks are steadily growing and increasing in severity.[3] It is thus no surprise that, in the UK's national security strategy, "hostile attacks upon UK cyber space by other states"[4] was labelled a "tier one risk" placing it at the very top of the British security agenda.

The threat of cyber attack has been met with a steady proliferation of strategies, policies and agencies attempting to secure cyberspace. Most states have a multi-tracked approach to cyber security, pursuing both international cooperation on cyber issues and at the same time seeking to build offensive capabilities in cyberspace. These Computer Network Operations (CNO) capabilities focus on deterrence. The discussion of deterrence in this brief will begin with an analysis of the nature of cyberspace in order to highlight some of the characteristics of the cyber realm which make deterrence problematic. The brief will then proceed to discuss the problems associated with cyber deterrence and ultimately argue that it is a 21st century Maginot Line.

The nature of cyberspace

Cyberspace is highly emblematic of the post-Westphalian international system. This system is to a large extent characterised by the demise of the traditional territorial sovereignty of the state.[5] The concept of sovereigns governing a territory with defined borders, as established by the Treaty of Westphalia in 1648 is increasingly being challenged by the growing interconnectedness and interdependence that exist between states today. Borders are blurring. Not only is cyberspace an integral part of this development, it is also a reflection of it. It is a borderless realm, ungoverned and unregulated – the equivalent of the 'wild west without a sheriff.' It is a Hobbesian construct where any governance regime requires the agreement of states with vastly differing perceptions of technology and the Internet. This is a key challenge to the multilateral approach to cyber security.

It is against this conceptual background that the Pentagon classified cyberspace as a battlespace in May 2009. As a battlespace, cyberspace has a set of defining characteristics that have important strategic implications for states: asymmetry, the attribution problem and lack of clear lines of division. All of these defining characteristics have important implications for the success of cyber deterrence.

[3] Baker, S., Fillipiak, N. and Timlin, K. (2011) *in the Dark*. Washington, D.C.: CSIS, p. 6.

[4] Her Majesty's Government (2010) *Britain in an Age of Uncertainty: The National Security Strategy*. London: Her Majesty's Stationery Office, p. 27.

[5] Hughes, R. (2010) "A Treaty for Cyberspace" *International Affairs*, 86:2, p. 535.

Cyberspace is highly asymmetrical. The low-cost and the relative ease with which offensive operations can be launched is staggering. An excellent illustration of this asymmetry on the tactical level is that of Iraqi insurgents who hacked the video feed of a Predator UAV using the software *Skygrabber,* purchased online for $25, which enabled them to view the video being transmitted back to its controllers. In this way, the insurgents were able to "evade or monitor US military operations."[6] Because the insurgents did not rely on any significant cyber infrastructure for the command and control system, the risk posed to them was at a minimum. According to the *Wall Street Journal,* the vulnerability was well known, "but the Pentagon assumed local adversaries wouldn't know how to exploit it (...)."[7] This underlines the fact that the Pentagon failed to grasp one further key characteristic of cyberspace: Technology, knowledge and know-how are available to anyone and non-proliferation is impossible. This element of instant proliferation further adds to the asymmetry of cyberspace.

The lack of attribution is a defining characteristic of the cyber realm. Unlike conventional warfare, the missiles of cyberspace do not carry flags, nor do they have traceable trajectories. It can be nearly impossible to attribute an attack to a certain actor. The Stuxnet worm is an excellent illustration of this. While there has been much media speculation as to who designed and deployed the worm against the Iranian nuclear programme, all attempts to effectively establish the origin of the weapon have been unsuccessful. Most likely, Stuxnet was designed with this in mind – as James P. Farwell and Rafal Rohozinski write: "Deliberate ambiguity is an effective shield against retribution."[8]

Lastly, the traditional dividing lines of society, i.e. between public and private and civil and military, are not clearly defined in cyberspace. Most of the military capabilities in cyberspace depend on privately-owned civilian infrastructure. An attacker might therefore wish to exclusively target civilian infrastructure. Some private actors, such as banks and other commercial enterprises, are reluctant to share information that could have a negative impact on their financial viability. Therefore, encroachments on national sovereignty might not be easily discovered.

Taken together, these characteristics of cyberspace form a wide array of challenges to cyber deterrence. Their strategic implications will be discussed further and applied to deterrence in the section below.

[6] Gorman, S., Dreazen, Y.J. and Cole, A. (2009) "Insurgents Hack U.S. Drones" *the Wall Street Journal*, 17 December 2009.

[7] Ibid.

[8] Farwell, J.P. and Rohozinski, R. (2011) "Stuxnet and the Future of Cyber War" *Survival*, p. 27.

Deterrence and Cyberspace – a Match Made in Heaven?

The threats stem from cyberspace and the daunting strategic implications of the battlespace described above bring to mind the advent of nuclear weapons in the early Cold War. Rather than being weapons of mass destruction, cyber weapons are weapons of mass disruption.[9] The success of deterrence during the Cold War was largely due to the nature of nuclear weapons. Deterrence theory offers two strategies available to states: denial and punishment. During the Cold War, both these strategies were applicable to nuclear deterrence. Nuclear technology could be denied to adversaries as demonstrated by the various legal non-proliferation regimes that are in place today. The development of second-strike capabilities, through for instance SLBM technology, enabled states to pursue a strategy of punishment, discouraging a first strike doctrine. The example of nuclear deterrence during the Cold War offers an attractive strategy in relation to cyberspace. Such a strategy would involve building capabilities that enable states to deny an adversary the advantage – by increasing the costs and risk of offensive operations.[10] However, in order for deterrence to be effective, several conditions must be met.

Criteria for successful deterrence in cyberspace

- **Capability:**
  States need to have the capability to respond, e.g. a well-established CNO capacity offering cyber instruments.
- **Signalling:**
  States need to signal their intent to retaliate, e.g. have doctrines and strategies in place which outline their intentions if they are attacked in cyberspace.
- **Credibility:**
  Along with cyber capabilities, states need to have targets available for retaliation, such as servers, cyber infrastructure or even physical objects in the event of a kinetic attack.

As outlined by Kenneth Geers,[11] denying an adversary the technical capability to conduct Computer Network Operations is virtually impossible due to the asymmetrical nature of cyberspace. The staggering speed of computer technology and the proliferation of it further underline the problems presented by a deterrence strategy based on denial.[12] Cyber deterrence based on punishment involves increasing the cost or risk of CNO to such a degree that it is rendered or deemed too costly to be pursued by an adversary.

A deterrence strategy based on punishment appears to be the order of the day among the leading states in the cyber domain. Such a strategy involves an element of the dictum that offence is the best defence. Several states pursue offensive operations in cyberspace and have created organisational and technical ca-

[9] Lamb, G. Gen. (2011) "Threat Now is From Weapons of Mass Disruption" *The Guardian*, 30 May 2011

[10] Kramer, F.D., Starr, S.H., Wentz, L.K. (2009) *Cyberpower and National Security*. Washinton, D.C.: National Defense University Press & Potomac Books, pp. 327-340

[11] Geers, K. (2010) "The Challenge of Cyber Attack Deterrence" *Computer Law & Security Review, 26(3)*, p. 301

[12] Ibid.

pabilities to support this strategy. *The Military Balance 2011,*[13] the authoritative annual assessment of global military capabilities, demonstrates how China, the United States, South Korea, Russia and the UK are seeking to develop offensive capabilities in cyberspace. *The Guardian* recently reported that: "The UK is developing a cyber-weapons programme that will give ministers an attacking capability to help counter growing threats to national security from cyberspace." The philosophy behind this strategy is also apparent in the establishment of the United States Cyber Command and the policy recommendations flowing into the White House. An example is CSIS' report on cyber security, in which it is recommended that the United States have "(...) a credible military presence in cyberspace (...)" and that "(...) possessing an offensive capability has a deterrence effect and the absence of an offensive capability makes deterrence a hollow threat."[14] During the presentation of the US Department of Defense's "Strategy for Operating in Cyberspace", General Cartwright said that he hoped that the Defense Department's cyber efforts will have moved from being 90% focused on defence to become 90% focused on deterrence within a decade. However, in order for such a strategy to succeed, a set of criteria has to be fulfilled. According to Geers, these criteria are: capability, signalling and credibility.[15]

In terms of capability, states might have the ability to respond to an attack. Nevertheless, if it is not possible to identify the attacker, this capability is rendered useless. Cyber forensics still has formidable challenges to overcome before the attribution problem can be solved. Equally, false flagging – the attempt to portray a third party as responsible for an attack – remains a problem. The much quoted Old Testament reference built into the code of Stuxnet is a good illustration of this.

If deterrence is to be successful, it is of paramount importance to signal the intention to retaliate. In terms of deterrence, the matter of military doctrine in cyberspace complicates matters further. Cyberspace is unique in that much of the critical infrastructure, such as power grids and transport control systems, are privately owned, and thus beyond the jurisdiction of governments. Some of the enterprises that rely on the trust of their customers might be reluctant to disclose an attack on their infrastructure for fear of the consequences. In order for deterrence to be effective, it is necessary to establish civil-military cooperation. Mostly likely, this will require regulation, which will probably not be welcomed by all industries.

At the very basic level, it is difficult to establish what constitutes an attack in cyberspace. The United States has declared that all options are open in a possible response to a cyber attack.[16] According to the *Wall Street Journal,* part of the fu-

[13] The International Institute for Strategic Studies (2011) *The Military Balance 2011.* London: Routledge, pp. 27-32

[14] Center for Strategic and International Studies (2008) *Securing Cyberspace for the 44th Presidency* Washington, D.C.: CSIS, p. 23

[15] Geers, K., op. cit.

[16] Baker, S., Filipiak, N. and Timlin, K., op. cit., pp. 16-17

ture strategy will be the notion of equivalence – a cyber attack that produces a level of destruction that is comparable to a conventional attack, which might result in a military response. As one source declared: "If you shut down our power grid, maybe we will put a missile down one of your smokestacks."[17] While such rhetoric might have a deterrent effect, the associated problems are vast – not least considering the attribution problem. Moreover, the wide array of actors in the cyber realm, such as hacktivists, 'online activists', and other non-state actors, could further complicate kinetic responses. This ambiguity underscores the limits of cyber deterrence.

The credibility of deterrence ties in with the asymmetrical nature of cyberspace. Considering the lack of territory in cyberspace, it is difficult to target an adversary. An illustration of the problem is the attack on Estonia. Even if the source of the attack was established with certainty, the computers used in the attack were mainly based in the United States and other states, including China. Retaliation thus became very difficult – while Estonia would be likely to gain the assistance of the United States, such help might not be forthcoming from states that Tallinn shared less trust with. Moreover, if the attacker is a non-state actor, their cyber infrastructure available for retaliation might be very limited. It is difficult to achieve deterrence because cyberspace is marked by such staggering asymmetry. In addition, the industrialised nations are more vulnerable due to their greater reliance on cyber infrastructure. A less developed state, such as North Korea, whose military infrastructure is largely independent of cyber infrastructure, could conduct offensive CNO without the same risks as most Western states.

This problem ties further in with the issues of escalating the level of belligerence. As a battlespace, on par with land, air, sea and space, cyberspace has a relatively low level of belligerence. If the problems of attribution and attack threshold are overcome, decision-makers are faced with the choice of how to respond. The United States has continuously argued for an approach that "[takes] nothing off the table" in terms of measure to respond.[18] Considering that both Britain and the United States have pledged to apply the Geneva Conventions (and the Law of Armed Conflict) to cyberspace,[19] it is essential to establish what constitutes an appropriate, proportional response to an attack in cyberspace.

While the idea of cyber deterrence is attractive, there are vast problems involved in building credible deterrence. The asymmetry, problems of attribution and threshold of attack along with the mix of public and private ownership all appear to make deterrence ineffective. On the other hand , the consequences of pursuing deterrence remain. Strategies that propel an overtly offensive element into cyberspace

[17] Barnes, J.E. and Gorman, S. (2011) "Cyberwar Plan Has New Focus on Deterrence" *The Wall Street Journal*, 15 July 2011

[18] Sanger, D.E. and Bumiller, E. (2011) "Pentagon to Consider Cyberattacks Acts of War" *New York Times*, 31 May 2011

[19] Ibid.; Harvey, N. (2011) "Forget a cyber Maginot Line" *The Guardian,* 30 May 2011

lead to a substantial risk of cyberspace being viewed as a zero-sum game, where the security gained by one state is at the expense of another. This threatens the stability of the networks upon which our societies rely. The alarm with which the United States views China's capabilities in cyberspace (and vice versa) is perhaps the most vivid illustration of this potential zero-sum game. During a congressional hearing on China's capabilities in cyberspace, the chairman of a congressional subcommittee opened his statement with the words: "The United States is under attack. Cyber- attacks and cyber espionage traced back to China have been dramatically increasing every year."[20]

Conclusion

The Maginot Line provided a false sense of security during a time of great anxiety. Cyber systems provide the backbone on which our technology-intensive societies rely. Critical infrastructure, the military command and control system and our knowledge economies all rely on a well-functioning cyber infrastructure. Any threat to this infrastructure is thus a top tier risk. The attack on Estonia in 2007, the theft of intellectual property related to the Joint Strike Fighter programme and the Stuxnet attack on the Iranian nuclear programme all highlight the urgent nature of the threat from cyberspace. These incidents have propelled a proliferation of government organisations and strategies to address the threat. An overarching element of these is deterrence and the development of offensive capabilities in cyberspace. This brief has demonstrated how cyber deterrence might very well be a 21st century Maginot Line, seemingly acting as a panacea to the threats stemming from the post-Westphalian realm of cyberspace. The reason for this is two-fold: the nature of cyberspace and owing to this, the limits of deterrence in the cyber realm. As a highly asymmetrical battlespace, cyberspace favours the advantage of the attacker. This condition is further reinforced by the lack of attribution, which ensures the anonymity of an attacker. As non-proliferation is impossible when it comes to software and hardware, the only remaining deterrence strategy available to states is punishment – to possess the offensive capability to punish an aggressor to such an extent that it deters them from attacking in the first place. Nonetheless, this brief has demonstrated why deterring an adversary is likely to be unsuccessful. Firstly, it is difficult to detect encroachments on national sovereignty due to the unwillingness of all actors to share information. Furthermore, there is no clearly determined threshold for identifying an incident as an attack. Secondly, deterrence relies on a credible retaliation capability. While technology-intensive states may offer an abundance of targets, most less developed states in the world do not. This argument is also particularly applicable to non-state actors whose infrastructure is often limited and ad hoc-based. In case of retaliation, a cyber attack could therefore prompt a kinetic response – and it is of paramount importance to deter-

[20] Dana Rohrabacher, 15 April 2011, hearing on Communist Chinese Cyber Attacks, Cyber espionage and the theft of American Technology, House of Representatives, Subcommittee on Oversight and Investigations, Committee on Foreign Affairs

mine the proportionality of this manoeuvre: Which kinetic response would shutting down the power grid merit? What if the attacker is a non-state actor? These are but a few questions that can be posed in relation to cyber deterrence. To continue down the road of cyber deterrence carries the risk that cyberspace becomes increasingly weaponised and viewed as a zero-sum security environment.

States should build operational capacities in the cyber domain, but it is unwise to perceive deterrence as a silver bullet. While applying the Law of Armed Conflict to cyberspace offers its own set of challenges, attempts should be made to mitigate the present anarchical nature of cyberspace. The sheriff needs to be brought into the cyber domain. This will undoubtedly require substantial diplomatic efforts that might not yield any result any time soon – but one thing remains clear: As technology continues to develop and become further integrated into our daily lives, the need for security in cyber systems becomes increasingly urgent. And therefore, the idea of a 21st century Maginot Line of cyber deterrence should not be pursued.